REMARKS

This paper is responsive to a Non-Final Office action dated May 15, 2007. Claims 1-3, 5-16, 18-22, 26-35, 37-43, and 45-57 were examined. Claims 1-3, 55, 6, 14-16, 18-22, 41-43, and 45-47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over "Applied Cryptography Protocols, Algorithms, and Source Code in C," by Bruce Schneier (hereinafter, "Schneier") in view of U. S. Patent Application Publication No. 2002/0094081 to Medvinsky (hereinafter, "Medvinsky"). Claims 7-13, 26-35, 37-40, and 48-51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of U. S. Patent Application Publication No. 2001/0052072 to Jung (hereinafter, "Jung"). Claims 7-13, 26-32, 34, 35, 37-40, and 48-51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Medvinsky and further in view of Jung. Claims 54-57 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Medvinsky, further in view of Jung, and further in view of U. S. Patent No. 6,918,034 to Sengodan et al. (hereinafter, "Sengodan").

Claim Rejections Under 35 U.S.C. § 103 Over Schneier in View of Medvinsky

Claims 1-3, 55, 6, 14-16, 18-22, 41-43, and 45-47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over "Applied Cryptography Protocols, Algorithms, and Source Code in C," by Bruce Schneier (hereinafter, "Schneier") in view of U. S. Patent Application Publication No. 2002/0094081 to Medvinsky (hereinafter, "Medvinsky"). Regarding claim 1, Applicants respectfully maintain that Schneier, alone or in combination with Medvinsky, or other references of record, fails to teach or suggest

> selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet,

as required by claim 1. Schneier teaches recovering plaintext bits from ciphertext using an XOR of bits of a key stream of index i and corresponding bits i of ciphertext, i.e., $p_i=c_i \oplus k_i$. §9.4. The XOR of corresponding bits of the key stream and ciphertext fails to teach or suggest selecting a fixed length segment of a continuous decryption key stream based on a received

session count of a data packet, as required by claim 1. Nowhere does Schneier teach or suggest that limitation of claim 1.

Medvinsky fails to compensate for the shortcomings of Schneier. Medvinsky teaches that

> processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

Paragraph 0033. Employing an RTP time stamp to calculate an index into a key stream to get appropriate key stream bytes for encryption of Medvinsky fails to teach or suggest selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet, as required by claim 1. Nowhere does Medvinsky teach or suggest selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet, as required by claim 1.

Since neither Schneier nor Medvinsky teaches or suggests the recited limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 1 and all claims dependent thereon, be withdrawn.

Regarding claim 48, Applicants respectfully maintain that Schneier, alone or in combination with Medvinsky, or other references of record, fails to teach or suggest

> a session count evaluator configured to determine if a difference between a received session count within the encrypted data packet and a locally generated session count is less than a threshold; and a decryption engine configured to decrypt the encrypted payload by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold,

as required by claim 48. Applicants respectfully point out that

> [o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. To facilitate this review, this analysis should be made explicit.

KSR Int'l Co. v. Teleflex Inc., 82 USPQ2d 1385, 1396 (U.S. 2007). The Office fails to point out where Schneier and Medvinsky teach the limitations of claim 48 and Applicants respectfully maintain that there is no apparent reason to combine the elements of Schneier and Medvinsky to teach the limitations of claim 48.

Schneier teaches producing a stream of ciphertext bits from plaintext bits using an XOR of bits of a key stream of index i and corresponding bits i of plaintext to generate ciphertext bits, i.e., $c_i=p_i \oplus k_i$. §9.4. "At the decryption end, the ciphertext bits are XORed with an identical key stream to recover the plaintext bits. $p_i=c_i \oplus k_i$." §9.4. The XOR of corresponding bits of the key stream and ciphertext fails to teach or suggest applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet, as required by claim 48. Nowhere does Schneier teach or suggest a decryption engine configured to decrypt the encrypted payload by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, as required by claim 48.

Medvinsky fails to compensate for the shortcomings of Schneier. Medvsinky teaches synchronization by directing key stream generator 132 to output the same key stream bytes from the same key stream used to encrypt the data by calculating an index into the key stream. Paragraph 0034. Nowhere does Medvinsky teach a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 48.

Since neither Schneier nor Medvinsky teaches or suggests the recited limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 48 and all claims dependent thereon, be withdrawn.

Regarding claim 14, Applicants respectfully maintain that Schneier, alone or in combination with Medvinsky, or other references of record, fails to teach or suggest

> selecting a fixed length segment of a continuous encryption key stream,

as required by claim 14. Schneier teaches producing a stream of ciphertext bits from plaintext bits using an XOR of bits of a key stream of index i and corresponding bits i of ciphertext, i.e., $p_i=c_i \oplus k_i$. §9.4. The XOR of corresponding bits of the key stream and ciphertext fails to teach or suggest selecting a fixed length segment of a continuous encryption key stream, as required by claim 14. Nowhere does Schneier teach or suggest that limitation of claim 14.

Medvinsky fails to compensate for the shortcomings of Schneier. Medvinsky teaches that

> processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

Paragraph 0033. Employing an RTP time stamp to calculate an index into a key stream to get appropriate key stream bytes for encryption of Medvinsky fails to teach or suggest selecting a fixed length segment of a continuous encryption key stream, as required by claim 14. Nowhere does Medvinsky teach or suggest selecting a fixed length segment of a continuous encryption key stream, as required by claim 14.

Since neither Schneier nor Medvinsky teaches or suggests the recited limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 14 and all claims dependent thereon, be withdrawn.

Regarding claim 41, Applicants respectfully maintain that Schneier, alone or in combination with Medvinsky, or other references of record, fails to teach or suggest

> an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to data to form an encrypted payload,

as required by claim 41. Schneier teaches producing a stream of ciphertext bits from plaintext bits using an XOR of bits of a key stream of index i and corresponding bits i of plaintext, i.e., $c_i=p_i \oplus k_i$. §9.4. The XOR of corresponding bits of the key stream and ciphertext fails to teach or suggest an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to data to form an encrypted payload, as required by claim 41. Nowhere does Schneier teach or suggest that limitation of claim 41.

Medvinsky fails to compensate for the shortcomings of Schneier. Medvinsky teaches that

> processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

Paragraph 0033. Employing an RTP time stamp to calculate an index into a key stream to get appropriate key stream bytes for encryption of Medvinsky fails to teach or suggest an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to data to form an encrypted payload, as required by claim 41. Nowhere does Medvinsky teach or suggest an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to data to form an encrypted payload, as required by claim 41.

Since neither Schneier nor Medvinsky teaches or suggests the recited limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 41 and all claims dependent thereon, be withdrawn.

Regarding claim 49, Applicants respectfully maintain that Schneier, alone or in combination with Medvinsky, or other references of record, fails to teach or suggest

> selecting a fixed length segment of a continuous decryption key stream based on the session count,

as required by claim 49. Schneier teaches recovering plaintext bits from ciphertext using an XOR of bits of a key stream of index i and corresponding bits i of ciphertext, i.e., $p_i=c_i \oplus k_i$. §9.4. The XOR of corresponding bits of the key stream and ciphertext fails to teach or suggest selecting a fixed length segment of a continuous decryption key stream based on the session count, as required by claim 49. Nowhere does Schneier teach or suggest that limitation of claim 49.

Medvinsky fails to compensate for the shortcomings of Schneier. Medvinsky teaches that

> processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

Paragraph 0033. Employing an RTP time stamp to calculate an index into a key stream to get appropriate key stream bytes for encryption of Medvinsky fails to teach or suggest selecting a fixed length segment of a continuous decryption key stream based on the session count, as required by claim 49. Nowhere does Medvinsky teach or suggest selecting a fixed length segment of a continuous decryption key stream based on the session count, as required by claim 49.

Since neither Schneier nor Medvinsky teaches or suggests the recited limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 49 and all claims dependent thereon, be withdrawn.

Regarding claim 53, Applicants respectfully maintain that Schneier, alone or in combination with Medvinsky, or other references of record, fails to teach or suggest

> selecting a fixed length segment of a continuous encryption key stream,

as required by claim 53. Schneier teaches producing a stream of ciphertext bits from plaintext bits using an XOR of bits of a key stream of index i and corresponding bits i of ciphertext, i.e., $c_i=p_i \oplus k_i$. §9.4. The XOR of corresponding bits of the key stream and plaintext fails to teach or suggest selecting a fixed length segment of a continuous encryption key stream, as required by claim 53. Nowhere does Schneier teach or suggest that limitation of claim 53.

Medvinsky fails to compensate for the shortcomings of Schneier. Medvinsky teaches that

> processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

Paragraph 0033. Employing an RTP time stamp to calculate an index into a key stream to get appropriate key stream bytes for encryption of Medvinsky fails to teach or suggest selecting a fixed length segment of a continuous encryption key stream, as required by claim 53. Nowhere does Medvinsky teach or suggest selecting a fixed length segment of a continuous encryption key stream, as required by claim 53.

Since neither Schneier nor Medvinsky teaches or suggests the recited limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 53 and all claims dependent thereon, be withdrawn.

Claim Rejections Under 35 U.S.C. § 103 Over Schneier in View of Jung

Claims 7-13, 26-35, 37-40, and 48-51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of U. S. Patent Application Publication No. 2001/0052072 to Jung (hereinafter, "Jung").

Regarding claim 33, Applicants respectfully maintain that Schneier, alone or in combination with Jung, or other references of record, fails to teach or suggest

> a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold; and a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold,

as required by claim 33. Schneier teaches recovering plaintext bits from ciphertext using an XOR of bits of a key stream of index i and corresponding bits i of ciphertext, i.e., $p_i=c_i \oplus k_i$. §9.4. The XOR of corresponding bits of the key stream and ciphertext fails to teach or suggest applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, as required by claim 33. Nowhere does Schneier teach or suggest that limitation of claim 33.

Jung fails to compensate for the shortcomings of Schneier. Jung teaches that "data must be decrypted in the same order or sequence in which it was encrypted." Paragraph 0013. Nowhere does Jung teach or suggest applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, as required by claim 33.

In addition, the Office action admits that Schneier fails to teach or suggest a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 33. The Office relies on paragraph 0013 of Jung to supply this teaching. This portion of Jung teaches that

> [a] requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized in order for the encryption and decryption to

> work properly. Specifically, the data must be decrypted in the same order or sequence in which it was encrypted. However, such synchronization is not only difficult to employ and maintain in the IP network 10, but can also consume a significant amount of bandwidth (e.g., 7-10% using RTP).

Paragraph 0013. Synchronization of a transmitter and a receiver, as taught by Jung fails to teach or suggest a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 33.

Since neither Schneier nor Jung teaches or suggests the recited limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 33 and all claims dependent thereon, be withdrawn.

Regarding claim 48, Applicants respectfully maintain that Schneier, alone or in combination with Jung, or other references of record, fails to teach or suggest

> a session count evaluator configured to determine if a difference between a received session count within the encrypted data packet and a locally generated session count is less than a threshold; and a decryption engine configured to decrypt the encrypted payload by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold,

as required by claim 48. As described above with regard to the combination of Schneier and Medvinsky, Schneier fails to teach or suggest applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, as required by claim 48.

Jung fails to compensate for the shortcomings of Schneier. Jung teaches that "data must be decrypted in the same order or sequence in which it was encrypted." Paragraph 0013. Nowhere does Jung teach or suggest applying a portion of a current fixed length segment of a

continuous decryption key stream to the data packet if the difference is less than the threshold, as required by claim 48.

In addition, the Office action admits that Schneier fails to teach or suggest a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 48. The Office relies on paragraph 0013 of Jung to supply this teaching. This portion of Jung teaches that

> [a] requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized in order for the encryption and decryption to work properly. Specifically, the data must be decrypted in the same order or sequence in which it was encrypted. However, such synchronization is not only difficult to employ and maintain in the IP network 10, but can also consume a significant amount of bandwidth (e.g., 7-10% using RTP).

Paragraph 0013. Synchronization of a transmitter and a receiver, as taught by Jung fails to teach or suggest a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 48.

Since neither Schneier nor Jung teaches or suggests the recited limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 48 and all claims dependent thereon, be withdrawn.

Regarding claim 49, Applicants respectfully maintain that Schneier, alone or in combination with Jung, or other references of record, fails to teach or suggest

> selecting a fixed length segment of a continuous decryption key stream based on the session count,

as required by claim 49. As described above with regard to the combination of Schneier and Medvinsky, Schneier fails to teach or suggest this limitation of claim 49. Jung fails to compensate for the shortcomings of Schneier. Jung teaches that "data must be decrypted in the same order or sequence in which it was encrypted." Paragraph 0013. Nowhere does Jung teach or suggest selecting a fixed length segment of a continuous decryption key stream based on the

session count, as required by claim 49. Since neither Schneier nor Jung teaches or suggests the recited limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 49 and all claims dependent thereon, be withdrawn.

Claim Rejections Under 35 U.S.C. § 103 Over Schneier in View of Medvinsky and Jung

Claims 7-13, 26-32, 34, 35, 37-40, and 48-51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Medvinsky and further in view of Jung.

Regarding claim 48, Applicants respectfully maintain that Schneier, alone or in combination with Medvinsky, Jung, and/or other references of record, fails to teach or suggest

> a session count evaluator configured to determine if a difference between a received session count within the encrypted data packet and a locally generated session count is less than a threshold; and a decryption engine configured to decrypt the encrypted payload by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold,

as required by claim 48. As described above with regard to the combination of Schneier and Medvinsky, Schneier and Medvinsky fail to teach or suggest applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, as required by claim 48. As described above with regard to the combination of Schneier and Jung, Jung fails to teach or suggest applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold, as required by claim 48. Since none of Schneier, Medvinsky, or nor Jung teaches or suggests the recited limitations and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 48 and all claims dependent thereon, be withdrawn.

Regarding claim 49, Applicants respectfully maintain that Schneier, alone or in combination with Jung, or other references of record, fails to teach or suggest

> selecting a fixed length segment of a continuous decryption key stream based on the session count,

as required by claim 49. As described above with regard to the combination of Schneier and Medvinsky, Schneier fails to teach or suggest this limitation of claim 49. Jung fails to compensate for the shortcomings of Schneier. As described above with regard to the combination of Schneier and Jung, Jung fails to teach or suggest selecting a fixed length segment of a continuous decryption key stream based on the session count, as required by claim 49. Since none of Schneier, Medvinsky, and Jung teaches or suggests the recited limitations and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 49 and all claims dependent thereon, be withdrawn.

Claim Rejections Under 35 U.S.C. § 103 Over Schneier in View of Medvinsky and Sengodan

Claims 54-57 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Medvinsky, further in view of Jung, and further in view of U. S. Patent No. 6,918,034 to Sengodan et al. (hereinafter, "Sengodan"). Applicants believe that claims 55-57 depend from allowable base claims and are allowable for at least this reason.

Regarding claim 54, Applicants respectfully maintain that Schneier, alone or in combination with Medvinsky, Jung, Sengodan, and/or other references of record, fails to teach or suggest

> padding the payload to a given size with padding, the given size corresponding to the fixed length segment size, wherein the fixed length segment of the continuous decryption key is applied to the padded payload, a remaining portion of the fixed length segment being applied to the padding,

as required by claim 54. The Office action admits that Schneier, Medvinsky, and Jung fail to teach that limitation of claim 54. The Office action relies on Sengodan to supply this teaching. Sengodan teaches

> assembling mini-packets into a payload wherein each mini-packet includes an associated mini-header for ensuring proper processing of each mini-packet and adding padding to mini-packets when the mini-packets are encrypted to insure each mini-packet is an integral multiple of a predetermined block size.

Col. 4, lines 31-36. Sengodan teaches further that

> First, a decision is made as to whether the mini-packet is encrypted 410. If the mini-packet is encrypted 420, padding is added. If the input (actual data) is of size "n" and the block size is "k", then the amount of padding "p" is given by: p=n-k*floor((n-1)/k).

Col. 8, lines 2-8. The amount of padding of Sengodan is variable and fails to teach or suggest padding the payload to a given size with padding, the given size corresponding to the fixed length segment size, as required by claim 54. In addition, Sengodan fails to describe a decryption key or a fixed length segment of a continuous decryption key. Nowhere does Sengodan teach or suggest that a fixed length segment of the continuous decryption key is applied to the padded payload, a remaining portion of the fixed length segment being applied to the padding, as required by claim 54. Since none of Schneier, Medvinsky, Jung, and Sengodan, alone or in combination, teaches or suggests the required limitation and no other art of record adds the missing disclosure, Applicants respectfully request that the rejection of claim 54 and all claims dependent thereon, be withdrawn.

Additional Remarks

Claim 35 is amended to correct a typographical error.

In summary, all claims are believed to be allowable over the art of record, and a Notice of Allowance to that effect is respectfully solicited. Nonetheless, if any issues remain that could be more efficiently handled by telephone, the Examiner is requested to call the undersigned at the number listed below.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that, on the date shown below, this correspondence is being

☐ deposited with the US Postal Service with sufficient postage as first class mail in an envelope addressed as shown above.

☐ facsimile transmitted to the USPTO.

☒ transmitted using the USPTO electronic filing system.

Nicole Teitler Cave — 8/15/07

Nicole Teitler Cave — Date

EXPRESS MAIL LABEL: _____

Respectfully submitted,

Nicole Teitler Cave, Reg. No. 54,021
Attorney for Applicant(s)
(512) 338-6315 (direct)
(512) 338-6300 (main)
(512) 338-6301 (fax)